Ekwan E. Rhow (CA SBN 174604)
erhow@birdmarella.com
Marc E. Masters (CA SBN 208375)
mmasters@birdmarella.com
Christopher J. Lee (CA SBN 322140)
clee@birdmarella.com
BIRD, MARELLA, RHOW, LINCENBERG, DROOKS & NESSIM, LLP
1875 Century Park East, 23rd Floor
Los Angeles, California 90067-2561
Telephone: (310) 201-2100
Facsimile: (310) 201-2110

Jonathan M. Rotter (CA SBN 234137)
Kara M. Wolke (CA SBN 241521)
Gregory B. Linkh (pro hac vice)
GLANCY PRONGAY & MURRAY, LLP
1925 Century Park East, Suite 2100
Los Angeles, California 90067-2561
Telephone: (310) 201-9150
jrotter@glancylaw.com
kwolke@glancylaw.com
glinkh@glancylaw.com

Attorneys for Plaintiffs

Kalpana Srinivasan (CA SBN 237460)
Steven Sklaver (CA SBN 237612)
Michael Gervais (CA SBN 330731)
SUSMAN GODFREY L.L.P.
1900 Avenue of the Stars
14th Floor
Los Angeles, CA 90067
Telephone: (310) 789-3100
ksrinivasan@susmangodfrey.com
ssklaver@susmangodfrey.com
mgervais@susmangodfrey.com

Y. Gloria Park (*pro hac vice*)
SUSMAN GODFREY L.L.P.
One Manhattan West
50th Floor
New York, NY 10001
Telephone: (212) 336-8330
gpark@susmangodfrey.com

John W. McCauley (*pro hac vice*)
SUSMAN GODFREY L.L.P.
1000 Louisiana Street, Suite 5100
Houston, TX 77002
Telephone: (713) 651-9366
Facsimile: (713) 654-6666
jmccauley@susmangodfrey.com

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

BERNADINE GRIFFITH; et al., individually and on behalf of all others similarly situated,

Plaintiffs,

vs.

TIKTOK, INC., a corporation; BYTEDANCE, INC., a corporation,

Defendants.

Case No. 5:23-cv-00964-SB-E

PLAINTIFFS' MEMORANDUM OF POINTS AND AUTHORITIES IN SUPPORT OF THEIR MOTION FOR CLASS CERTIFICATION

REDACTED VERSION OF DOCUMENT PROPOSED TO BE FILED UNDER SEAL

JUDGE: Hon. Stanley Blumenfeld, Jr.
DATE: August 16, 2024
COURTROOM:
U.S. Courthouse
350 West 1st Street
Los Angeles, CA 90012
Courtroom 6C

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Rules

I. INTRODUCTION

In 2022, Congress took TikTok to task for falsely representing that "TikTok does not track users' internet data while not using the application." Ex. to Park Decl. ("Ex.") 1. Specifically addressing the TikTok Pixel ("Pixel"), two ranking members warned that "TikTok is clandestinely gathering some of Americans' most sensitive internet history, regardless of whether they use the application or not." *Id.* Undeterred, TikTok, Inc. ("TikTok") and its sister company, ByteDance, Inc. (together "Defendants"), continue to deploy the Pixel and its partner tool, Events API, to secretly record the online activity of millions of U.S. residents who never registered for a TikTok account ("class members").

The Pixel is a piece of software that companies can embed on their websites. Defendants market the Pixel to advertisers as a tool that allows their advertising on the TikTok platform to be more effective by allowing TikTok to collect data on the advertisers' website visitors through the Pixel and then use that data to personalize the ads that those visitors see while on the TikTok app.[1] Today, hundreds of thousands of websites have the Pixel installed. Problematically, the Pixel cannot differentiate between a TikTok user and a non-user, which means that Defendants do not limit their data collection to website visitors who are TikTok users; they indiscriminately collect a default baseline of data from ***all*** website visitors. That data collected includes [redacted] and substantively sensitive data on non-TikTok users—all taken without their knowledge or consent. Sample Pixel data produced by Defendants [redacted]. *See infra* at Sec. III.C.1.a. Defendants also added default Pixel functions to auto-scrape websites for

[1] For background on pixels generally and the TikTok Pixel, see the Shafiq Declaration ("Shafiq"), ¶¶25-37.

metadata and infer class members' button clicks to track their every movement around a webpage. Ex. 2; Shafiq ¶56.

Privately, Defendants admit that [redacted]. Defendants acknowledge that [redacted] Ex. 3 at -2934. But they continue to collect class member data anyway because [redacted], and they have not [redacted] Ex. 8 (215:2-20). [redacted] Ex. 4 at -3015, with [redacted] Ex. 5 at -125349. Defendants continue to intrude on class members' privacy, knowing that doing so is unnecessary and disproportionate to their services, because [redacted].

Defendants' conduct presents common issues that permeate each cause of action. Classwide proof will show that Defendants collected default data fields from class members as they engaged with every website that installed the Pixel. Common evidence also will show that Defendants did not disclose their data collection to class members and failed to obtain their consent. And common evidence—including Defendants' own admissions—confirms that Defendants used class members' data for their own profit.

Plaintiffs seek to hold Defendants accountable. Plaintiffs respectfully request that the Court certify the proposed classes and subclasses set forth in the accompanying Motion. Class 1 seeks to represent all non-TikTok users whose data Defendants intercepted from websites that use the Pixel.[2] Class 2 seeks to represent the subset of Class 1 whose data Defendants intercepted from websites that use both the Pixel and Events API. Class 3 consists of the subset of Class 1—and Class 4 consists of the subset of Class 2—who had their browser or system settings

[2] For each class, Plaintiffs propose a corresponding California resident subclass.

configured to block third-party cookies. Finally, Class 5 consists of the subset of Class 1 where the websites from which data was intercepted did not have the "Search" event configured for their Pixel. In the alternative, Plaintiffs seek to certify the website-specific classes and subclasses (Classes 6-10).

II. LEGAL STANDARD

To be certified, a proposed class must satisfy Rule 23(a)'s prerequisites and at least one of Rule 23(b)'s three prongs. *Ruiz Torres v. Mercer Canyons Inc.*, 835 F.3d 1125, 1132 (9th Cir. 2016). Certification is appropriate if: "(1) the class is so numerous that joinder of all members is impracticable; (2) there are questions of law or fact common to the class; (3) the claims or defenses of the representative parties are typical of the claims or defenses of the class; and (4) the representative parties will fairly and adequately protect the interests of the class." Fed. R. Civ. P. 23(a).

Plaintiffs seek certification under two prongs of Rule 23(b): an injunctive class pursuant to Rule 23(b)(2) and a damages class pursuant to Rule 23(b)(3). Rule 23(b)(2) requires that "the party opposing the class has acted or refused to act on grounds that apply generally to the class, so that final injunctive relief or corresponding declaratory relief is appropriate respecting the class as a whole." Fed. R. Civ. P. 23(b)(2). Rule 23(b)(3) requires that "questions of law or fact common to class members predominate over any questions affecting only individual members, and that a class action is superior to other available methods for fairly and efficiently adjudicating the controversy." Fed. R. Civ. P. 23(b)(3).

III. ARGUMENT

A. California Law Governs Plaintiffs' Non-Federal Claims.

All claims but the Federal Wiretap Act ("ECPA") claim arise under California law. *Mazza v. Am. Honda Motor Co.*, 666 F.3d 581 (9th Cir. 2012), sets "the framework for applying California law to a nationwide class action." *Kearney v. Hyundai Motor Am.*, 2012 WL 13049699, at *7 (C.D. Cal. Dec. 17, 2012). Once the class action proponent carries its initial burden of demonstrating that California has

"significant contact or significant aggregation of contacts" to class claims, "the burden shifts to the other side to demonstrate that foreign law, rather than California law, should apply to class claims." *Id.* (quoting *Mazza*, 666 F.3d at 589).

Plaintiffs easily satisfy their initial burden. TikTok maintains global headquarters in California and publicizes that its California office accommodates its over 400 US employees, including "key leadership hires." Dkt. 147 at ¶11; Exs. 6, 35. [redacted]. Ex. 8 (37:3-19). [redacted]. Ex. 7 (42:14-21); Ex. 8 (32:5-19, 33:25-34:8); Ex. 9 (43:16-44:17, 114:13-17). Moreover, TikTok has selected California law to govern its agreements with TikTok users and advertisers located nationwide. *See* Exs. 10, 11.

Courts have applied California law nationwide in similar circumstances. *See, e.g.*, *Rodriguez v. Google, LLC*, 2024 WL 38302, at *13 (N.D. Cal. Jan. 3, 2024) (certifying nationwide classes for California invasion of privacy and intrusion upon seclusion claims); *Doe v. Meta Platforms, Inc.*, 690 F.Supp.3d 1064, 1079 (N.D. Cal. 2023) (applying CIPA "extraterritorially" because "plaintiffs have plausibly alleged that the conduct at issue, in terms of the design and marketing of the Pixel technology and development and implementation of its Terms of Service, occurred in California"); *Parkinson v. Hyundai Motor Am.*, 258 F.R.D. 580, 599 (C.D. Cal. 2008) (applying California law to nationwide class).

B. The Proposed Class Satisfies the Rule 23(a) Requirements.

Numerosity. Rule 23(a)(1) requires that a class be "so numerous that joinder of all members is impracticable." "[W]hen a proposed class has at least forty members, joinder is presumptively impracticable based on numbers alone." *In re*

Banc of California Sec. Litig., 326 F.R.D. 640, 646 (C.D. Cal. 2018). Here, the Classes and Subclasses contain millions, if not tens of millions, of members. Shafiq ¶¶ 36, 95.

Commonality. The requirement to show common questions of fact and law is not an onerous one: "a single common question" will do. *See Franklin v. Midwest Recovery Sys., LLC*, 2021 WL 1035121, at *2 (C.D. Cal. Feb. 5, 2021). Rule 23(a)(2)'s requirements have "been construed permissively," and "[a]ll questions of fact and law need not be common to satisfy the rule." *Ellis v. Costco Wholesale Corp*, 657 F.3d 970, 981 (9th Cir. 2011) (citation omitted). Here, the same common issues that establish predominance under Rule 23(b)(3) also establish commonality. *Comcast Corp. v. Behrend*, 569 U.S. 27, 34 (2013); *see infra* at Sec. III.C.

Typicality and Adequacy. Typicality requires that the plaintiffs' claims be typical of the class "to assure that the interest of the named representative aligns with the interests of the class." *Hanon v. Dataprods. Corp*., 976 F.2d 497, 508 (9th Cir. 1992). The requirement is "permissive," and the representative's claims need only be "reasonably co-extensive with those of absent class members." *Hanlon v. Chrysler Corp*., 150 F.3d 1011, 1020 (9th Cir. 1998), *overruled on other grounds by Wal-Mart Stores, Inc. v. Dukes*, 564 U.S. 338 (2011). Typicality is satisfied here:

- During the Class Period, each Named Plaintiff visited websites using the Pixel and Events API,[3] has never had a TikTok account, and has had their web browser or system settings turned on to block third-party cookies. They will represent Classes 1-5. Each will also represent nationwide classes (Classes 6-10, in the alternative) based on which particular websites they visited.
- Ms. Griffith has resided in California since at least March 2022. Ms. Shih resided in California until earlier this year. They will represent applicable California subclasses.

Griffith, Shih, Watters Decls; *see* Mot. at 4-5.

[3] [redacted]. *Se*

For substantially the same reasons, and as stated in their declarations, Plaintiffs will adequately represent the proposed classes. *Woods v. Vector Mktg. Corp*., 2015 WL 5188682, at *12 (N.D. Cal. Sept. 4, 2015) ("typicality and adequacy inquiries tend to significantly overlap"). Further, there is no "conflict[] of interest with other class members." *Staton v. Boeing Co*., 327 F.3d 938, 957 (9th Cir. 2003). Likewise, counsel will adequately represent the classes as demonstrated by their commitment to date. *See* Rhow, Rotter, Gervais Decls.

C. Plaintiffs Satisfy Rule 23(b)(3)'s Predominance Requirement for a Damages Class.

Predominance "requires a showing that *questions* common to the class predominate, not that those questions will be answered, on the merits, in favor of the class." *Amgen, Inc. v. Conn. Retirement Plans & Trust Funds*, 568 U.S. 455, 459 (2013). The rule "does *not* require" that each element of a plaintiffs' claim be susceptible to classwide proof. *Id.* at 469. "When 'one or more of the central issues in the action are common to the class and can be said to predominate, the action may be considered proper under Rule 23(b)(3) even though other important matters will have to be tried separately.'" *Tyson Foods, Inc. v. Bouaphakeo*, 577 U.S. 442, 453 (2016) (citation omitted). "Merits questions may be considered to the extent—but only to the extent—that they are relevant to determining" whether class certification is appropriate. *Amgen*, 568 U.S. at 466.

1. Common Issues Predominate for the Invasion of Privacy and Intrusion Upon Seclusion Claims.

Courts often consider these claims together and ask whether "(1) there exists a reasonable expectation of privacy, and (2) the intrusion [on privacy] was highly offensive." *In re Facebook, Inc. Internet Tracking Litig.* ("*FB Tracking*"), 956 F.3d 589, 601 (9th Cir. 2020). This is an objective, "reasonable person" standard. *Rodriguez*, 2024 WL 38302, at *4. It does "not require individualized determinations

of class members' subjective expectations." *Opperman v. Path*, 2016 WL 3844326 at *11 (N.D. Cal. Jul. 15, 2016).

a. Class Members Have a Reasonable Expectation of Privacy

To determine whether a reasonable privacy expectation exists, courts ask "whether a defendant gained 'unwanted access to data by electronic or other covert means, in violation of the law or social norms.'" *FB Tracking*, 956 F.3d at 601 (citation omitted). The relevant question is whether a non-TikTok user would reasonably expect that TikTok collects her data from non-TikTok websites. *See Griffith*, 2023 WL 7107262 at *5.

The answer, which is "no," is the same for all class members. Class members "have never used the TikTok app or registered for a TikTok account." *Id.* at *2. As they have not registered for TikTok accounts, they were never informed by TikTok of anything. Nor were they informed by the websites: The privacy policies of Rite-Aid, Hulu, Etsy, and Upwork, for example, do not even mention Defendants, let alone disclose that data is being shared with either entity. Exs. 12-18. Sweetwater's policy references TikTok once in an inapposite context. Ex. 32.

Given Defendants' "customs, practices and circumstances surrounding [their] particular activities," *FB Tracking*, 956 F.3d at 602, it is unsurprising that websites did not disclose that class members' data was collected by Defendants. Common evidence will show that Defendants outsourced the obligation to disclose data collection by the Pixel and Events API to the websites themselves via boilerplate language in their Business Products (Data) Terms that "[y]ou must only share with us or enable us to collect Business Products Data in a manner that is transparent and lawful" and that "[y]ou . . . must therefore have provided all necessary transparency notices, and have all necessary rights, permissions and lawful bases (including consent, if and where required) required by applicable laws." Ex. 31.

Classwide proof will demonstrate that Defendants [redacted]. In one [redacted], Defendants

acknowledge that [redacted]. Ex. 19 at -9052 [redacted]). Defendants acknowledge that they [redacted] *Id.* While Defendants pay lip service to consent and disclosure, they do [redacted] *Id.* at -9053. Given that neither the websites nor Defendants disclosed the data collection to class members, class members had an objective, reasonable expectation of privacy that their data was not being collected by TikTok through non-TikTok websites. This is especially true for the cookie-blocking classes, where class members affirmatively set their browsers to block third-party cookies, objectively showing that they did not want third parties, like Defendants, to collect their data.

Common evidence will show that, without class members' consent, Defendants collected and continue to collect class members' data using uniform "electronic or other covert means." *FB Tracking*, 956 F.3d at 602-03. They do so in two ways. First, they use the Pixel, embedded on non-TikTok websites. With the Pixel, Defendants automatically collect the following seven categories of data from Class Members: Timestamp, IP Address, User Agent, Cookies, URL, Event Information, and Content Information ("Default Data"). Shafiq ¶¶47-66. Critically, this Default Data is collected from all websites using the Pixel—regardless of what specific events the websites choose to collect data on, how the websites configure the Pixel, and the web browser with which website visitors are visiting the page. Indeed, Plaintiffs' expert Dr. Shafiq preliminarily tested thousands of websites with the Pixel—pulled from TikTok's own data—and confirmed that the Default Data categories are uniformly collected. *Id.* at ¶¶76-80. Similarly, Dr. Shafiq's testing demonstrates that the browser used by class members makes no difference to the Pixel's data collection. *Id.* at ¶¶81-86. In short, the Pixel's automatic collection of

Default Data is uniform across class members. And Defendants' own documents confirm that this has been the case since at least March 2022 when the most recent of the Default Data categories—Cookies—became a default. Ex. 20 at -249.

Second, Defendants use Events API, a server-to-server tool, to collect class members' data substantially similar to that collected through the Pixel. Shafiq. ¶¶38-46. Events API was [redacted]. *See, e.g.*, Ex. 21 at -140-41.

Common evidence will show that the Default Data contain [redacted] and substantively sensitive information. [redacted]. Ex. 7 (294:6-295:3). Meanwhile, the URL—which includes both Page URL (the full URL of the webpage the website visitor is viewing) and Referrer URL (the full URL of the preceding webpage from which the visitor navigated to the current webpage)—is [redacted] and sensitive. As explained by Dr. Shafiq, in even the small sample of collected data that Defendants have produced to date, the [redacted]

[redacted] *See id*.

In addition to [redacted]. *See FB Tracking*, 956 F.3d at 603 (considering sensitivity of data collected as part of reasonable-expectation-of-privacy inquiry). For instance, [redacted] Shafiq ¶63. Likewise, when one searches for "pregnancy test" on riteaid.com, Defendants collect the following URL: https://www.riteaid.com/shop/catalogsearch/result/?q=pregnancy%20test. *Id.* These search term-embedded URLs are collected alongside the other automatically collected identifiers, which enables Defendants to match an identity with the sensitive search term.

Finally, the Pixel automatically collects "Event Information" and "Content Information" about what website visitors are doing, viewing, and clicking on a webpage. Based on Dr. Shafiq's testing, the Pixel automatically collects information about the precise sequence of actions performed by a class member on a website with the Pixel deployed. Shafiq ¶56.

The amount of class-member data collected through the Pixel is staggering. *See FB Tracking*, 956 F.3d at 603 (considering amount of data collected as part of reasonable-expectation-of-privacy inquiry). Defendants themselves have represented that a mere "24-hour snapshot of the data [it collects] would consist of billions of rows and trillions of data points" and "would be over **50 terabytes** of data." Dkt. 103 at 2-3; *see* Shafiq ¶36 (collecting public and internal estimates on the scale of Pixel's data collection). [redacted] *See* Shafiq ¶37 (discussing Defendants' documents [redacted]).

At bottom, class members here are analogous to the plaintiffs in *FB Tracking*, who objectively indicated their desire not to be tracked by Facebook by logging out

of Facebook, 956 F.3d at 602, and to the plaintiffs in *Rodriguez*, who objectively indicated their desire not to have their browsing data saved by Google by turning off a "Web & App Activity" button, 2024 WL 38302, at *5. Class members here similarly chose not to be tracked by TikTok by not registering for TikTok. Indeed, like in *Rodriguez*, the evidence of class members' reasonable expectation of privacy (not having a TikTok account) is not only subject to common proof but also built into the class definition. *Cf. Samson v. United Healthcare Servs. Inc.*, 2023 WL 6793973, at *10 (W.D. Wash. Oct. 13, 2023).

b. Defendants' Intrusion Is Highly Offensive

The second element—whether Defendants' privacy intrusion is highly offensive to a reasonable person—is also subject to common proof. This test focuses on the "degree to which the intrusion is unacceptable as a matter of public policy." *FB Tracking*, 956 F.3d at 606. The factors considered are common to the class: the "degree and setting of the intrusion," the "intruder's motives and objectives," the intruder's own recognition that its practices are "a problematic privacy issue," and "the degree to which the intrusion is unacceptable as a matter of public policy." *Id.*

The **degree and setting of Defendants' intrusion** is uniform classwide. For all class members, Defendants used the Pixel and Events API to intrude into their Internet browsing, and Defendants have automatically collected the same set of Default Data.

Common evidence will also show Defendants' **own recognition of the privacy issues** created by their conduct. Defendants internally [redacted]. Their documents discuss how Pixel data [redacted]

[redacted] Ex. 3 at -2934, 2938 (emphasis added). Elsewhere, one employee asks: [redacted] Ex. 22 at -9195. In yet another document, an employee [redacted] Ex. 4 at -3033. Defendants even [redacted] Ex. 23 at -8759.

Beyond the recognition of the sensitive nature of Pixel data, common evidence will show that Defendants [redacted] Ex. 30 at -9008. Indeed, Defendants [redacted] Ex. 3 at -2934.

Undeterred by these privacy concerns, Defendants continued to collect massive amounts of class members' data with the "**motives and objectives**" of (1) continuing [redacted], and (2) [redacted]. *See* Ex. 24 at -9921 ([redacted]). First, common evidence (Defendants' own documents) reveals [redacted]. *See, e.g.*, Ex. 4 at -3015; Ex. 34 at -9850. To build out their Pixel [redacted]. *See* Ex. 8 (215:2-20) (Defendants' corporate representative testifying [redacted]).

Second, Defendants directly used the collected class member data in its own right. Ex. 3 at -2938. TikTok stated publicly that "[i]f TikTok receives data about someone who doesn't have a TikTok account, the company only uses the data for aggregated reports that they send to advertisers about their websites." Ex. 33. Internal documents [redacted] *Id.* at -2932. Interrogatory responses confirm that [redacted] Ex. 25.

Finally, common evidence will show that Defendants' intrusion is highly offensive because it is surreptitious. Defendants actively conceal the extent of the Pixel's data collection, for instance, by failing to disclose URL as being collected automatically. Shafiq ¶33 & n.57. Defendants' practices are also becoming *more* surreptitious over time. TikTok previously disclosed on its website that "[b]y default, the pixel base code will always include page view events which measure when a person lands on any of your webpages." That disclosure is gone. *Compare* Ex. 26 at -132, *with* Ex. 27. TikTok previously disclosed the existence of the PixelBot, which "automatically scans and analyzes keywords on your public website to help classify and contextualize your content." Ex. 28. That disclosure is gone. *See* Shafiq ¶¶35, 65(iii)-(iv).

2. Common Issues Predominate for the ECPA Claim.

ECPA prohibits attempted and actual interceptions of any "electronic communication." 18 U.S.C. §§ 2511(1)(a)-(d). "Plaintiffs must show that [Defendants] (1) intentionally (2) intercepted (3) the contents of (4) plaintiffs' electronic communications (5) using a device." *In re Meta Pixel Healthcare Litig.*, 647 F.Supp.3d 778, 794-95 (N.D. Cal. 2022). Common evidence will show that Defendants (1) intentionally (2) intercepted data between class members and non-

TikTok websites (5) using a device. Indeed, the technical functioning of the Pixel and Events API turns on common questions and are subject to common proof. *See supra* at Sec. III.C.1.a; Shafiq ¶¶30-66.

The URLs automatically collected by Defendants constitute (3) the contents of (4) plaintiffs' electronic communications. *See Meta Pixel*, 647 F.Supp.3d at 795 ("descriptive URLs" that "include both the 'path' and the 'query string'" are "contents" under ECPA); *In re Google RTB Consumer Privacy Litig.*, 606 F.Supp.3d 935, 949 (N.D. Cal. 2022) (ECPA "contents" include "URL of the page where the impression will be shown" and "referrer URL that caused navigation to the current page"); *Brown v. Google LLC*, 685 F.Supp.3d 909, 936 (N.D. Cal. 2023) (search queries are like "the contents of a letter").

The ECPA claim is appropriate for classwide resolution. *See Harris v. comScore, Inc.*, 292 F.R.D. 579, 585, 590 (N.D. Ill. 2013) (certifying ECPA claim where "the software attempts to collect the same information from all computers, and the question of whether that collection exceeds the scope of consent is common to all plaintiffs").

3. Common Issues Predominate for the CIPA Claims.

Plaintiffs assert claims under sections 631 and 632 of CIPA. Section 631(a) "prohibits the unauthorized interception of 'any message, report or communication.'" *Brown v. Google LLC*, 525 F.Supp.3d 1049, 1073 (N.D. Cal. 2021). It has four requirements: the defendant (1) willfully (2) "reads, or attempts to read, or to learn the contents" of a "message, report, or communication" (3) while the communication is "in transit"; and (4) "without the consent of all parties." Cal. Penal Code § 631(a); *Valenzuela v. Nationwide Mut. Ins. Co.*, 686 F.Supp.3d 969, 976-77 (C.D. Cal. 2023). Section 631(a) applies to communications over the internet. *Javier v. Assurance IQ, LLC*, 2022 WL 1744107, at *1 (9th Cir. May 31, 2022).

The first three elements focus entirely on Defendants' conduct and are subject to classwide proof. *See In re Yahoo Mail Litig.*, 308 F.R.D. 577, 591 (N.D. Cal. 2015)

(whether technical process by which "Yahoo intercepts emails" satisfies CIPA is a "common contention" that is "capable of classwide resolution"). Defendants learned the contents of intercepted communications between websites and website visitors by willfully designing and marketing the Pixel so that certain data, including URLs, is collected by default. Whether URLs constitute "contents" under CIPA is also a question common to the class. *See Gershzon v. Meta Platforms, Inc.*, 2023 WL 5420234, at *13 (N.D. Cal. Aug. 22, 2023) (CIPA's "contents" requirement satisfied where "the Pixel transmits to Meta the URL of each page visited on a website"); *Meta Pixel*, 647 F.Supp.3d at 795-96, 798. Likewise, the Pixel's transmission of data to Defendants constitutes an interception because "a first party [the website visitor] intends to communicate with a second party [the website], and computer code [the Pixel] automatically directs the communications to an additional third party [Defendants]." *Valenzuela*, 686 F.Supp.3d at 976. This interception also happens while the data is "in transit." Shafiq ¶¶32, 67 (TikTok [redacted]); *id.* at ¶41 (same for Events API).

Finally, class members did not consent to or authorize Defendants' interception of their communications with websites. *Supra* at Sec. III.C.1.a; *infra* at Sec. III.C.6.

Section 631(a) separately prohibits the "use" or attempted use of improperly intercepted information. *Valenzuela*, 686 F.Supp.3d at 979. The evidence of Defendants' use of class members' data is uniform classwide. *Supra* at Sec. III.C.1.b.

The Section 632 claim is also appropriate for classwide resolution. Section 632(a) applies to the eavesdropping or recording "of a *confidential* communication," meaning "one of the parties 'has an objectively reasonable expectation that the conversation is not being overheard or recorded.'" *Meta Pixel*, 647 F.Supp.3d at 798 (citation omitted). For the reasons discussed above, *see supra* Sec. III.C.1.a, class

members have an objectively reasonable expectation that the data that they share with non-TikTok websites are not being intercepted and collected by TikTok.

4. Common Issues Predominate for the Conversion Claim.

"The elements of a conversion are the plaintiff's ownership or right to possession of the property at the time of the conversion; the defendant's conversion by a wrongful act or disposition of property rights; and damages." *Roley v. Google LLC*, 2020 WL 8675968, at *11 (N.D. Cal. Jul 20, 2020) (certifying class for conversion claim). Plaintiffs will demonstrate through common evidence that Defendants collect a common set of data from class members that constitutes their property. *See CTC Real Est. Servs. v. Lepe*, 140 Cal.App.4th 856, 860 (Cal. Ct. App. 2006) (PII can be "object of theft" and is a "valuable asset"). Whether class members had a right to possess their data or consented to its taking is a legal question that will be resolved together for all members. Whether Defendants' data collection is "wrongful" will also turn on common evidence showing their collection of data without consent using invasive, highly offensive means. *See supra* Sec. III.C.1. Because class members share a common objective expectation of privacy as individuals who did not register for TikTok accounts and because Defendants used the same illegal means to collect data from each member, the conversion claim is appropriate for classwide resolution.

5. Common Issues Predominate for the Statutory Larceny Claim.

California law forbids obtaining property "in any manner constituting theft." Cal. Penal Code § 496. Theft includes "feloniously steal[ing], tak[ing], carry[ing], lead[ing], or driv[ing] away the personal property of another." *Id.* at § 484. Defendants commit theft by larceny where they "(1) take[] possession (2) of personal property (3) owned or possessed by another, (4) by means of trespass and (5) with intent to steal the property, and (6) carries the property away." *People v. Davis*, 19 Cal.4th 301, 305 (1998). Trespass, in turn, simply means "[t]he act of taking personal property from the possession of another." *Id.* Once again, whether class members'

data constitutes property is a common legal question that should be adjudicated classwide. And whether Defendants "trespassed" on that property is subject to common proof through Defendants' documents and Dr. Shafiq's analysis that explains how the Pixel and Events API function to collect data.

6. Common Issues Predominate as to Defendants' Consent Defense.

To the extent that Defendants oppose certification on the ground that class members consented to Defendants' data collection, such a defense is meritless. "In order for consent to be actual, the disclosures must 'explicitly notify' users of the practice at issue." *Google RTB*, 606 F.Supp.3d at 949 (*citing In re Google, Inc.*, 2013 WL 5423918, at *12 (N.D. Cal. Sept. 26, 2013)). This requires notices of the "specific practice." *Campbell v. Facebook, Inc.*, 77 F.Supp.3d 836, 848 (N.D. Cal. 2014). A "generalized notice is not sufficient to establish consent." *Meta Pixel*, 647 F.Supp.3d at 793.

Defendants outsource the disclosure obligation to the websites that use the Pixel and Events API, [redacted] *See supra* Sec. III.C.1.a. To date, Defendants have failed to produce evidence of any website using Pixel or Events API that expressly notifies class members of Defendants' data collection.

In any event, as demonstrated by Dr. Shafiq's testing, the Pixel fires and begins to automatically collect the Default Data discussed above ***as soon as*** the visitor lands on the URL and ***before*** he had a chance to do ***anything*** on that webpage, like click on a disclosure or cookie-usage consent button. Shafiq ¶¶77-78 (describing how Pixel collected data from 2,000 randomly selected webpages, using automation software that visited each site without simulating any user interactions).

7. Common Issues Predominate for the Monetary Relief Sought.

The requested monetary relief is "'capable of measurement on a classwide basis,' in the sense that the whole class suffered damages traceable to the same injurious course of conduct." *Just Film, Inc. v. Buono*, 847 F.3d 1108, 1120 (9th Cir.

2017) (quoting *Comcast*, 569 U.S. at 34-35); *Pulaski & Middleman*, 802 F.3d 979, 986 (9th Cir. 2015) ("'damage calculations alone cannot defeat certification'" (citation omitted)).

a. Disgorgement of Profits

The invasion of privacy, intrusion upon seclusion, and ECPA claims all allow for recovery in the form of disgorgement of profits resulting from unjust enrichment. *Rodriguez*, 2024 WL 38302, at *11 (permitting disgorgement remedy for intrusion upon seclusion and invasion of privacy claims); 18 U.S.C § 2520(c)(2)(A) ("any profits made by the violator as a result of the violation"). The amount of Defendants' unjust enrichment is a common issue and will be proven with common evidence. Plaintiffs' damages expert, Dr. Mangum, puts forth two different methodologies to calculate disgorgement of profits attributable to the Pixel and Events API. The first is by quantifying the value that Defendants derive from using the class member data collected through these tools. Mangum ¶¶54-57.

The second is by calculating the value of the Pixel and Events API to Defendants. *Id.* at ¶¶58-84. As Defendants' corporate representative admitted, they [redacted]. Ex. 8 (215:2-20). Given this admission, [redacted] Dr. Mangum explains how he can calculate the value of the Pixel—or the incremental advertising revenue earned by Defendants as a result of the Pixel—using common evidence, namely Defendants' own internal financial documents (that are the subject of pending discovery requests). Mangum ¶¶58-60. Even if Defendants (improperly) refuse to produce their financials, however, Dr. Mangum can calculate the profits to be disgorged through Defendants' documents [redacted] and other internal valuations. *Id.* Using this common evidence, Dr. Mangum can extrapolate Defendants' revenue attributable to the Pixel during the Class Period, *id.* at ¶¶60-74, and adjust the

revenues to account for the fraction of the global revenue that is attributable to U.S. class members, *id*. at ¶¶70-71. The same methodology can be used to calculate Defendants' revenue attributable to Events API. *Id.* at ¶¶75-83; Ex. 29.

b. Actual or Restitutionary Damages

The conversion, statutory larceny, and ECPA claims allow for restitutionary damages. Cal. Civ. Code § 3336; *Switzer v. Wood*, 35 Cal.App.5th 116, 119 (2019); 18 U.S.C § 2520(c)(2)(A) ("the sum of the actual damages suffered by the plaintiff"). Actual damages can be calculated classwide using common evidence. Dr. Mangum can calculate the damages by quantifying the amount of payments necessary to compensate class members for the market value of the data that Defendants collected from them. Mangum ¶¶85-89. To do so, Dr. Mangum can rely on classwide evidence, namely the amounts that (1) corporations like Google, Nielsen, and SavvyConnect have paid consumers for data comparable to that collected through the Pixel and Events API, and (2) corporations like Meta and AT&T have charged consumers to opt out from their comparable data being collected. *Id.* at ¶¶90-123. In *Rodriguez*, the court certified a 23(b)(3) damages class based in part on similar methodology, using similar data sources, that calculated actual damages by referencing the amounts that Google paid for user data. 2024 WL 38302, at *11-12.

c. Statutory Damages

ECPA and CIPA provide for statutory damages. Cal. Penal Code § 637.2(a); 18 U.S.C § 2520(c)(2)(B). "Statutory damages are calculated as prescribed by the statutes. What the statute provides is a common question of law, so common questions predominate for the damages analysis, too." *Kellman v. Spokeo, Inc*., 2024 WL 2788418, at *11 (N.D. Cal. May 29, 2024). Dr. Mangum can calculate the damages number consistent with the statutory prescriptions. Mangum ¶¶124-125.

d. Punitive and Nominal Damages

Punitive damages are available for the invasion of privacy, intrusion upon seclusion, and ECPA claims. *Condon v. Condon*, 2008 WL 11338437, at *7 (C.D.

Cal. June 6, 2008). Because "the purpose of punitive damages is not to compensate the victim, but to punish and deter the defendant, . . . the focus of a punitive damages claim is 'not on facts unique to each class member, but on the defendant's conduct toward the class as a whole.'" *Ellis v. Costco Corp. III*, 285 F.R.D. 492, 542 (N.D. Cal. 2012) (citations omitted) (certifying Rule 23(b)(3) class including claim for punitive damages); *Rodriguez*, 2024 WL 38302, at *7 ("At this [class certification] juncture, 'it is sufficient to decide that the availability of punitive damages is amenable to class wide resolution,' through common evidence." (citation omitted)).

D. Class Action Is a Superior Method of Adjudicating Plaintiffs' Claims.

A class action here will achieve "economies of time, effort, and expense" and promote "uniformity of decision as to persons similarly situated." *Amchem Prods. v. Windsor*, 521 U.S. 591, 615 (1997) (citation omitted). With millions of potential class members, a "class action promotes efficiency and judicial economy." *Franklin*, 2021 WL 1035121, at *8. It would be inefficient and cost prohibitive to litigate millions of claims individually rather than on a classwide basis.

E. Plaintiffs Need Not Demonstrate Administrative Feasibility of Identifying Class Members to Obtain Class Certification.

Class members can self-identify. *Kellman*, 2024 WL 2788418, at *11. "[P]laintiffs may use the claims administration process to determine which claimants belong in which classes, using common evidence . . . to determine class membership." *Id.* at *15. Eric Schachter, Plaintiffs' expert on class notice and administration, puts forth a robust approach to provide notice to class members. *See* Schachter ¶¶8-34. "Post-judgment claims forms and other tools can be used to allow defendants to test a class member's purported entitlement to damages and to apportion damages appropriately between class members." *In re Lidoderm Antitrust Litig.*, 2017 WL 679367, at *25 (N.D. Cal. Feb. 21, 2017) (citing *Briseno v. ConAgra Foods, Inc.*, 844 F.3d 1121, 1131 (9th Cir. 2017)).

F. Rule 23(b)(2) Certification Is Also Warranted.

Plaintiffs seek certification under Rule 23(b)(2) with respect to Plaintiffs' claims for injunctive and declaratory relief.[4] Rule 23(b)(2) certification is appropriate where plaintiffs challenge centralized policies that do not require individualized injunctive relief. *See B.K. by next friend Tinsley v. Snyder*, 922 F.3d 957, 971 (9th Cir. 2019). Courts do not examine the viability of class members' claims for declaratory and injunctive relief, "but only [] look at whether class members seek uniform relief from a practice applicable to all of them." *Ward v. United Airlines, Inc.*, 2021 WL 534364, at *7 (N.D. Cal. Feb. 12, 2021).

Plaintiffs seek injunctive relief to (1) preclude Defendants from collecting class members' data through the Pixel or Events API, (2) require Defendants to delete all class members' data, (3) require Defendants to discontinue all features, offerings, and services that they developed or improved using class members' data, and (4) appoint an independent third party to verify that the injunctive relief has been implemented. This requested relief is sufficiently detailed at this juncture. Rule 23(b)(2) "ordinarily will be satisfied when plaintiffs have described the general contours of an injunction that would provide relief to the whole class, that is more specific than a bare injunction to follow the law, and that can be given greater substance and specificity at an appropriate stage in the litigation." *Parsons v. Ryan*, 754 F.3d 657, 689 n.35 (9th Cir. 2014).

"Unlike Rule 23(b)(3), a plaintiff does not need to show predominance of common issues or superiority of class adjudication to certify a Rule 23(b)(2) class." *Yahoo Mail Litig.*, 308 F.R.D. at 587 (certifying injunctive relief class requesting Yahoo to stop scanning emails and explaining that Yahoo's "focus on whether a potential class member has consented to Yahoo's [conduct] loses sight of the purpose

[4] The Court may certify claims under both 23(b)(3) and 23(b)(2). *In re Xyrem (Sodium Oxybate) Antitrust Litig.*, 2023 WL 3440399, at *12 (N.D. Cal. May 12, 2023).

of Rule 23(b)(2)," *id.* at 599); *DZ Rsrv. v. Meta Platforms, Inc*., 2022 WL 912890, at *9 (N.D. Cal. Mar. 29, 2022).

G. If the Court Does Not Certify Under Rule 23(b)(2) or (b)(3), Certification of Particular Issues is Appropriate Under Rule 23(c)(4).

Even if predominance is not satisfied as to the "entire action," Rule 23(c)(4) permits the Court to "isolate the common issues" and "proceed with class treatment of these particular issues." *In re Apple iPhone Antitrust Litig*., 2022 WL 1284104, at *17 (N.D. Cal. Mar. 29, 2022) (citation omitted). If the Court finds that any claims are ill-suited for (b)(3) or (b)(2) certification, Plaintiffs respectfully submit there are numerous issues appropriate for classwide determination under Rule 23(c)(4). The issues Plaintiffs propose (in the alternative) to certify under Rule 23(c)(4) are key elements of their claims, and include whether:

- The Pixel and Events API each operates to collect data of class members that visit websites unaffiliated with TikTok, including certain baseline data automatically collected regardless of the websites' own configurations;
- Whether and by how much Defendants were unjustly enriched from the Pixel's and/or Events API's unauthorized data collection;
- Whether class and subclass members suffered lost value of their PII as a result of the Pixel's and/or Events API's unauthorized data collection.

These key issues can be resolved with common evidence in the form of expert testimony and the documents and data produced in this case.

IV. CONCLUSION

Plaintiffs request that the Court certify both 23(b)(3) and 23(b)(2) classes, appoint Plaintiffs as class representatives, and Plaintiffs' counsel as class counsel.

Dated: June 21, 2024

By: /s/ *Ekwan E. Rhow*

Ekwan E. Rhow (CA SBN 174604)
Marc E. Masters (CA SBN 208375)
Christopher J. Lee (CA SBN 322140)
BIRD, MARELLA, RHOW, LINCENBERG, DROOKS & NESSIM, LLP
1875 Century Park East, 23rd Floor

Los Angeles, California 90067-2561
Telephone: (310) 201-2100
erhow@birdmarella.com
mmasters@birdmarella.com
clee@birdmarella.com

Jonathan M. Rotter (CA SBN 234137)
Kara M. Wolke (CA SBN 241521)
Gregory B. Linkh (*pro hac vice*)
GLANCY PRONGAY & MURRAY, LLP
1925 Century Park East, Suite 2100
Los Angeles, California 90067-2561
Telephone: (310) 201-9150
jrotter@glancylaw.com
kwolke@glancylaw.com
glinkh@glancylaw.com

Kalpana Srinivasan (CA SBN 237460)
Steven Sklaver (CA SBN 237612)
Michael Gervais (CA SBN 330731)
SUSMAN GODFREY L.L.P.
1900 Avenue of the Stars, Suite 1400
Los Angeles, CA 90067
Telephone: (310) 789-3100
Facsimile: (310) 789-3150
ksrinivasan@susmangodfrey.com
ssklaver@susmangodfrey.com
mgervais@susmangodfrey.com

Y. Gloria Park (pro hac vice)
SUSMAN GODFREY L.L.P.
One Manhattan West
50th Floor
Telephone: (212) 336-8330
Facsimile: (310) 336-8340
gpark@susmangodfrey.com

John W. McCauley (*pro hac vice*)
SUSMAN GODFREY L.L.P.
1000 Louisiana Street, Suite 5100
Houston, TX 77002
Telephone: (713) 651-9366
Facsimile: (713) 654-6666
jmccauley@susmangodfrey.com

Attorneys for Plaintiffs

CERTIFICATE OF COMPLIANCE

The undersigned counsel of record for Plaintiffs certifies that this brief contains 6,982 words, which complies with the word limit of L.R. 11-6.1.

Dated: June 21, 2024

By: /s/ *Ekwan E. Rhow*
Ekwan E. Rhow

Attorneys for Plaintiffs